UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/528,456	03/17/2000	Martin Kienzle	YOR000028US1	4380

7590   10/06/2003

Frank Chau Esq
F. Chau & Associates LLP
1900 Hempstead Turnpike
Suite 501
East Meadow, NY 11554

EXAMINER
BOWES, SARA E

ART UNIT	PAPER NUMBER
2171	

DATE MAILED: 10/06/2003

3

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *3/17/2000* .

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

     4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *3/17/2000* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

     If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

     a)☐ All b)☐ Some * c)☐ None of:

         1.☐ Certified copies of the priority documents have been received.

         2.☐ Certified copies of the priority documents have been received in Application No. _____ .

         3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

     * See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

     a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)   4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)   5) ☐ Notice of Informal Patent Application (PTO-152)

3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *2* .   6) ☐ Other: .

DETAILED ACTION

Drawings

The drawings are objected to under 37 CFR 1.83(a). The drawings must show every feature of the invention specified in the claims. Therefore, the memory storage device of claims 7, 13, 19, 25, and 31 and the steganographically embedding step of claims 16, 22, and 28 must be shown or the feature(s) canceled from the claim(s). No new matter should be entered.

A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Objections

Applicant is advised that should claim 19 be found allowable, claim 31 will be objected to under 37 CFR 1.75 as being a substantial duplicate thereof. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

Claim Rejections - 35 USC § 112, First Paragraph

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the

art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 10, 16, 22, and 28 rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Referring to claim 10, the specification does not describe steganographically hiding the encryption key in the first unit, it only discusses hiding the key in the second unit.

Referring to claims 16, 22, and 28, the specification does not describe embedding portions of the encryption key in the at least one first unit with respect to the base claims of the above claims. The specification does discuss embedding portions of the encryption key in the first and second units.

Claim Rejections - 35 USC § 112, Second Paragraph

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1 and 8 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1 and 8 are rejected as being incomplete for omitting essential elements, such omission amounting to a gap between the elements. See MPEP § 2172.01.

Referring to claim 1, the omitted element is a connection between the scrambler

and the steganographic unit.

Referring to claim 8, the omitted element is a connection between the key

extractor and the descrambler.

Claims 1 and 8 are rejected for being inconsistent. Claim 1 recites a scrambler

for encrypting at least one first unit using an encryption key and a steganographic unit

for embedding the encryption key into at least one second unit. However, claim 8

recites a key extractor for extracting an encryption key steganographically hidden in at

least one first unit and a descrambler for descrambling at least one second unit. This

inconsistence between claims 1 and 8 makes the scope of the claim indeterminate.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of

the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of

the various claims was commonly owned at the time any inventions covered therein

were made absent any evidence to the contrary. Applicant is advised of the obligation

under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was

not commonly owned at the time a later invention was made in order for the examiner to

consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g)

prior art under 35 U.S.C. 103(a).

Claims 1, 2, 6-13, 16-20, 22-26, 28-31, 33, and 34 are rejected under 35 U.S.C.

103(a) as being unpatentable over Ichikawa to U.S. Patent 5,872,846 in view of Orrin to

U.S. Patent 6,011,849.

Referring to claim 1, 20, and 33 Ichikawa teaches a system and method

comprising a server [see Figure 5, Sender, 502] coupled to a transmission link for

providing a data stream to at least one client [see Figure 5, Receiver, 516] over the

transmission link [see Figure 5, Transmission], the data stream being segmented into

units, the server including a scrambler for encrypting at least one first unit using an

encryption key [see Figure 5, Encryption and Receiver's Public key, 508].

Ichikawa does not teach a system or method of a server comprising a

steganographic unit for embedding the encryption key into at least one second unit for

the data stream such that steganographic information is needed by the client to

determine the encryption key and decipher the data stream.

However, Orrin does teach a system and method of a server comprising a

steganographic unit for embedding the encryption key into at least one second unit [see

Figure 4, and column 4, lines 45-47].

It would have been obvious to one of ordinary skill in the art at the time the

invention was made to modify Ichikawa to include the steganographic teachings of

Orrin. Namely, inserting a steganographic unit in the "sender terminal" 502 of Figure 5

[see Ichikawa]. One of ordinary skill in the art would have been motivated to modify

Ichikawa as above for the purpose of improving the security of the encrypted data to be transmitted over an unsecured communication line.

Referring to claim 2, Ichikawa as modified by Orrin teaches a steganographic unit employing a steganographic masking algorithm [see column 4, lines 39-40 of Orrin].

Referring to claim 4, Ichikawa as modified by Orrin teaches steganographic unit encrypts the at least one second unit [see column 4, lines 52-63 of Orrin].

Referring to claims 5, 11, 17, 23, and 29, Ichikawa as modified by Orrin teaches at least one first unit and the at least one second unit are encrypted and each carries a portion of the encryption key [see column 8, lines 44-58 of Orrin].

Referring to claims 6, 12, 18, 24, and 30, Ichikawa as modified teaches a transmission link including the Internet [see column 3, lines 30-32].

Referring to claims 7, 13, 19, 25, and 31, Ichikawa as modified teaches at least one of the client and the server including a memory storage device [see Figure 5, Receiver's Public Key, 508 and Receiver's Private Key, 520 and column 5]. In order for the sender [server] and receiver [client] to use the private and public keys of the receiver there must be a memory device to store the keys.

Referring to claims 8, 26, and 34, Ichikawa teaches a system and method comprising a client system coupled to a transmission link for receiving a data stream to at least one server over the transmission link, the data stream being segmented into units, the client system including a descrambler for descrambling at least one second unit which was encrypted in accordance with the encryption key before transmission from the server [see Figure 5, Decryption and Receiver's Private Key, 520].

Ichikawa does not teach a system or method of a client comprising:

- a key extractor for extracting an encryption key steganographically hidden in at

  least one first unit in the data stream received from the server such that

  steganographic information is needed by the client to determine the encryption

  key; and

- a decoder coupled to the key extractor and the descrambler for reassembling the

  data stream such that all of the units of the data stream are needed to decipher

  the data stream.

However, Orrin does teach a system and method of a client comprising:

- a key extractor for extracting an encryption key steganographically hidden in at

  least one first unit in the data stream received from the server such that

  steganographic information is needed by the client to determine the encryption

  key [see column 9, lines 13-16]; and

- a decoder coupled to the key extractor and the descrambler for reassembling the

  data stream such that all of the units of the data stream are needed to decipher

  the data stream [see column 9, lines 16-19].

Also refer to column 9, lines 34-42 of Orrin for further explanation.

It would have been obvious to one of ordinary skill in the art at the time the

invention was made to modify Ichikawa to include the key extractor and the decoder of

Orrin. Namely, inserting the key extractor and the decoder in the "receiver terminal" 516

of Figure 5 [see Ichikawa]. One of ordinary skill in the art would have been motivated to

modify Ichikawa as above for the purpose of providing a higher level of secure to

encrypted data being transmitted over an unsecured transmission line.

Referring to claim 10, Orrin as modified teaches hiding the encryption key is also

steganographically hidden in the at least one second unit [see Figure 4 and column 4,

lines 45-55].

Referring to claims 16, 22, and 28, Orrin as modified teaches the step of

steganographically embedding portions of the encryption key in the at least one first unit

[see column 8, lines 44-58].

Claims 3, 9, 14, 15, 21, 27, and 32 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Ichikawa in view of Orrin, and further in view of Katta et al.

Referring to claims 3, 9, 15, 21, and 27, Ichikawa and Orrin teach all limitations of

the aforementioned claims except for the data stream including a transmission order,

which alternates between first units and second units.

Katta et al. disclose a data stream including a transmission order, which

alternates between first units and second units [see Figure 3 and column 3, lines 16-19].

It would have been obvious to one of ordinary skill in the art at the time the

invention was made to modify Ichikawa and Orrin to include the transmission order of

Katta et al. Namely, inserting a multiplexer at the output of the "sender terminal" 502 of

Figure 5 [see Ichikawa]. One of ordinary skill in the art would have been motivated to

modify Ichikawa and Orrin as above for the purpose of improving the security of the

data stream by separating the data into the data packets making the entire program

[movie, music files, etc.] more difficult to decrypt.

Referring to claims 14 and 32, Ichikawa teaches a method comprising:

- providing data to be transmitted over a link [see Figure 5, Transmission];

- scrambling at least one first unit by encrypting the at least one first unit using an encryption key [see Figure 5, Encryption and Receiver's Public key, 508]; and

- descrambling at least one first unit which was encrypted in accordance with the encryption key [see Figure 5, Decryption and Receiver's Private Key, 520].

Ichikawa does not teach a method comprising:

- steganographically embedding the encryption key into at least one second unit for the data stream such that steganographic information is needed by a client to determine the encryption key and decipher the data;

- extracting the encryption key steganographically embedded in the at least one second unit in the data stream;

- reassembling the data steam at the client such that all of the units of the data stream are needed to decipher the data stream.

However, Orrin does disclose a method comprising:

- steganographically embedding the encryption key into at least one second unit for the data stream such that steganographic information is needed by a client to determine the encryption key and decipher the data stream [see Figure 4, and column 4, lines 45-47];

- extracting the encryption key steganographically embedded in the at least one second unit in the data stream [see column 9, lines 13-16];

- reassembling the data steam at the client such that all of the units of the data stream are needed to decipher the data stream [see column 9,lines 16-19].

However, neither Ichikawa nor Orrin explicitly teach segmenting the data into units for a data stream to be transferred over the line.

Katta et al does teach segmenting the data into units for a data stream to be transferred over the line [see Figure 3 and column 3, lines 16-19].

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Ichikawa to include the teachings of Orrin. Namely combining the subsystems of claims 1[the server system] and 8 [the client system]. One of ordinary skill in the art would have been motivated to modify Ichikawa as above for the purpose of producing a secure, compatible server client network.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined teachings of Ichikawa and Orrin to include the teaching of Katta et al. Namely, inserting a multiplexer at the output of the "sender terminal" 502 of Figure 5 [see Ichikawa]. One of ordinary skill in the art would have been motivated to modify Ichikawa and Orrin as above for the purpose of improving the security of the data stream by separating the data into the data packets making the entire program [movie, music files, etc.] more difficult to decrypt.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 6,038,316 to Dwork et al.

U.S. Patent No. 5,790,666 to Ooi.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sara Bowes whose telephone number is 703-305-0326. The examiner can normally be reached on 7:30-4:00, Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Safet Metjahic can be reached on 703-308-1436. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

seb
9/30/03

SAFET METJAHIC
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100